What is claimed is:

1. A method of processing encryption data in a computing entity said method characterized by comprising steps of:

assigning a memory means of said computing entity into a plurality of memory areas (710);

receiving encrypted data (720);

storing said encrypted data in a first memory area of said computing entity (720), said first memory area assigned for use by a kernel code of an operating system of said first computing entity;

writing said encrypted data stored in said first memory area into a second memory area associated with said computing entity (730);

decrypting said encrypted data stored in said second memory area (740); and

writing said decrypted data from said second memory area to said first memory area (750).

2. A method as claimed in claim 1, wherein said first memory area is logically distinct from said second memory area.

3. A method as claimed in claim 1, wherein said first memory area is configured to contain code of said operating system.

4. The method as claimed in claim 1, wherein said second memory area is not used for storage of code of a kernel of said operating system.

5. The method as claimed in claim 1, wherein said step of decrypting said encrypted data stored in said second area is carried out by an internet security protocol program resident in said second memory area.

6. A method of processing encryption data in a computing entity said method characterized by comprising steps of:

assigning a memory means of said computing entity into a plurality of memory areas (810);

storing decrypted data in a first said memory area of said plurality of memory areas, said first memory area being assigned for use by a kernel code of an operating system of said first computing entity (820);

writing said stored data into a second memory area of said plurality of memory areas associated with said first communicating entity (830);

encrypting said data stored in said second memory area (840); and

writing said encrypted data from said second memory area to said first memory area (850).

7. A method as claimed in claim 6, wherein said first memory area is logically distinct from said second memory area.

8. A method as claimed in claim 6, wherein said first memory area is configured to contain code of said operating system.

9. A method as claimed in claim 6, wherein said second memory area is not used for storage of code of a kernel of said operating system.

10. A method as claimed in claim 8, further comprising the step of redirecting said encrypted data from said operating system in said first memory area to an encryption/decryption stack resident in said second memory area.

11. A method as claimed in claim 9, comprising the step of directing said data to said second memory area from said first memory area.

12. A method as claimed in claim 6, wherein said step of encrypting said data stored in said second memory area is carried out by an internet protocol security program stored in said second memory area.

13. A method of processing encrypted data in a computing entity, said computing entity comprising;

a processor; and

a memory means,

wherein said memory means is divided into first and second memory areas, wherein said first memory area contains code of an operating system of said computer entity, said method comprising the steps of:

receiving an encrypted data packet;

processing said data packet according to at least one packetization protocol of said operating system in said first memory area;

outputting said data packet to said second memory area;

processing said data packet according to a decryption algorithm in said second memory area; and

returning said processed data packet to said operating system in said first memory area.

14. A digital computer configurable for transmitting digital data across a communications network, said digital computer comprising;

at least one microprocessor unit (530);

a memory means, wherein said memory means is logically sub divided into at least a first memory area (508) and a second memory area (520) and characterized by further comprising;

a redirection means (503) for writing data from said first memory area (500) to said second memory area (520) and from said second memory area to said first memory area; and

encryption means (509) logically located within said second memory area, said encryption means configurable for encrypting said digital data.

15. A digital computer configurable for receiving digital data transmitted across a communications network, said digital computer comprising:

at least one microprocessor unit (530);

a memory means, wherein said memory means is assigned into at least a first memory area (500) and a second memory area (520) and characterized by further comprising;

a redirection means (503) for writing data from said first memory area (500) to said second memory area (520) and from said second memory area (520) to said first memory area (500); and

decryption (509) means logically located within said second memory area (520) for decrypting data stored in said second memory area (520), said decryption means (509) being configurable for decrypting said data.

16. A digital computer as claimed in claim 15, wherein said redirection means comprises;

a redirection layer (503); and

a port for interfacing said redirection layer and said encryption means (504).

17. A digital computer as claimed in claim 15, wherein said encryption means logically located within said second memory area comprises:

an internet protocol security stack (509); and

a database configurable to contain key data (605) for encrypting said data.

18. A digital computer as claimed in claim 15, wherein said encryption means logically located within said second memory area comprises:

a plurality of internet protocol security stacks (1210, 1220); and

a plurality of data bases (1260, 1270) configurable to contain key data for encrypting said data, wherein each data base of said plurality of databases contains a same key data.

19. A digital computer as claimed in claim 18, wherein said plurality of internet protocol security stacks are generated using a plurality of computing languages.

20. A computing entity comprising:

a data processing means;

a memory means;

an operating system having a set of kernel code, containing a communications protocol stack code;

a plurality of encryption and decryption means;

a first area of said memory means being assigned to said operating system code;

a second area of said memory means being assigned to said plurality of encryption and decryption means, said second memory area being sub-assigned into a plurality of compartmented memory areas within said second memory area, wherein individual ones of said encryption and decryption means are resident in corresponding respective ones of said plurality of compartmented memory areas.

21. The computing entity as claimed in claim 20, further comprising a director means resident in said first memory area, said director means arranged to input data from and output data to said communications protocol stack.

22. The computing entity as claimed in claim 21, wherein said director means sends a plurality of data streams to said plurality of compartmented memory areas and receives a plurality of data streams from said plurality of compartmented memory areas.

23. The computing entity as claimed in claim 21, wherein said director means operates to send a corresponding respective data stream to each of said plurality of compartmented memory areas, and receive said corresponding respective data stream from said corresponding compartmented memory areas.

24. The computing entity as claimed in claim 20, further comprising a plurality of ports resident in said first memory area, there being at least one said port per said compartmented memory area, said port positioned between a said corresponding respective compartmented memory area, and a director means for directing data streams to and from said plurality of compartmented memory areas, said director means being resident in said first memory area.

25. The computing entity as claimed in claim 20, comprising a plurality of data processor means, said plurality of data processors providing processing capability for carrying out data processing operations within said plurality of compartmented memory areas.

26. A method of encryption processing a plurality of packet data streams between first and second layers of a communications protocol stack, said method comprising the steps of:

receiving a first said data packet stream from a first layer of said protocol stack in a first memory area;

sending said data packet stream to a first compartmented memory area;

running an encryption process on said first data packet stream in said first compartmented memory area for encryption or decryption of said data packet stream;

returning said processed data packet stream from said first compartmented memory area to a second layer of said communications protocol stack in said first memory area;

receiving a second packet data stream from a said first or second layer of said communications protocol stack in said first memory area;

sending said second data packet stream to a second compartmented memory area;

encryption processing said second data packet stream in said second compartmented memory area for encryption or decryption of said data packet stream; and

returning said processed second packet data stream to the other one of said first or second said layers of said communications protocol stack in said first memory area,

wherein said first compartmented memory area is assigned to said first process, said second compartmented memory area is assigned to said second

process, and said first memory area is assigned to an operating system of said computing entity.

27. The method as claimed in claim 26, comprising the step of running a plurality of processes in a said compartmented memory area, for processing a single said packet data stream.